Amendments to the Claims

Claim 1 (currently amended): In a computing environment having a connection to a network, a computer program product for securely propagating security credentials using a trusted authenticating domain, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);

computer-readable program code means for transmitting an identifier of a user and an identifying secret of the user from the client to the PSA over the secure connection;

computer-readable program code means for validating the user with the trusted authenticating domain using the transmitted user identifier and identifying secret, on request of the PSA; and

computer-readable program code means for propagating the identifying secret of the user directly from the PSA to a master registry if the validation succeeds.

Claim 2 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a second secure connection between the PSA and the trusted authenticating domain; and

computer-readable program code means for using the second secure connection for the validating of the user.

Claim 3 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a third secure connection between the PSA and the master registry; and

computer-readable program code means for using the third secure connection for the propagating of the identifying secret to the master registry.

Claim 4 (original): The computer program product according to Claim 1, further comprising computer-readable program code means for propagating the identifying secret to one or more other target registries if the validation succeeds.

Claim 5 (original): The computer program product according to Claim 4, further comprising:

computer-readable program code means for establishing additional secure connections between the PSA and each of the other target registries; and

computer-readable program code means for using the additional secure connections for the propagating of the identifying secret to the other target registries.

Claim 6 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining an identification of the trusted authenticating domain from the user; and

computer-readable program code means for verifying that the trusted authenticating domain is trusted by the master registry as a prerequisite to the propagating.

Claim 7 (original): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining an identification of the trusted authenticating domain from the master registry.

Claim 8 (original): The computer program product according to Claim 6, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-readable program code means for checking whether the stored trust policy information for the user includes the identification obtained from the user.

as Claim 9 (original): The computer program product according to Claim 6, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-readable program code means for checking whether the stored trust policy information for a user group of which the user is a member includes the identification obtained from the user.

Claim 10 (original): The computer program product according to Claim 7, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises computer-readable program code means for obtaining the identification using the stored trust policy information for the user.

Claim 11 (original): The computer program product according to Claim 7, wherein the master

registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises computer-readable program code means for obtaining the identification using the stored trust policy information for a user group of which the user is a member.

Claim 12 (original): The computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret to the one or more other target registries further comprises computer-readable program code means for identifying the one or more other target registries using the stored password synchronization policy information for the user.

Claim 13 (original): The computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret to the one or more other target registries further comprises computer-readable program code means for identifying the one or more other target registries using the stored password synchronization policy information for a user group of which the user is a member.

Claim 14 (original): The computer program product according to Claim 1, wherein the computer-readable program code means for establishing the secure connection further comprises computer-readable program code means for authenticating the PSA to the client.

Claim 15 (original): The computer program product according to Claim 2, wherein the computer-readable program code means for establishing the second secure connection further comprises computer-readable program code means for authenticating the trusted authenticating domain to the PSA.

Claim 16 (original): The computer program product according to Claim 3, wherein the computer-readable program code means for establishing the third secure connection further comprises computer-readable program code means for authenticating the master registry to the PSA.

Claim 17 (original): The computer program product according to Claim 5, wherein the computer-readable program code means for establishing additional secure connections further comprises computer-readable program code means for authenticating the other target registries to the PSA.

Claim 18 (currently amended): The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises:

computer-readable program code means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

computer-readable program code means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the trusted authenticating domain; and

computer-readable program code means for concluding that the validation succeeds if comparing the located identifying secret is identical to a result of performing the security function.

Claim 19 (original): The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises computer-readable program code means for invoking an authenticated LDAP bind or other native authentication mechanism of the trusted authenticating domain, wherein the identifier of the user and the identifying secret of the user are passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

Claim 20 (original): The computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the master registry.

Claim 21 (original): The computer program product according to Claim 4, wherein the PSA has administrative authority for performing operations at the one or more other target registries.

Claim 22 (currently amended): A system for securely propagating security credentials using a trusted authenticating domain, comprising:

means for establishing a secure connection between a client and a password synchronization agent (PSA);

means for transmitting an identifier of a user and an identifying secret of the user from the

client to the PSA over the secure connection;

means for validating the user with the trusted authenticating domain using the transmitted user identifier and identifying secret, on request of the PSA; and

means for propagating the identifying secret of the user directly from the PSA to a master registry if the validation succeeds.

Claim 23 (original): The system according to Claim 22, further comprising:

means for establishing a second secure connection between the PSA and the trusted authenticating domain; and

means for using the second secure connection for the validating of the user.

Claim 24 (original): The system according to Claim 22, further comprising:

means for establishing a third secure connection between the PSA and the master registry; and

means for using the third secure connection for the propagating of the identifying secret to the master registry.

Claim 25 (original): The system according to Claim 22, further comprising means for propagating the identifying secret to one or more other target registries if the validation succeeds.

Claim 26 (original): The system according to Claim 25, further comprising:

means for establishing additional secure connections between the PSA and each of the

other target registries; and

means for using the additional secure connections for the propagating of the identifying secret to the other target registries.

Claim 27 (original): The system according to Claim 22, further comprising:

means for obtaining an identification of the trusted authenticating domain from the user; and

means for verifying that the trusted authenticating domain is trusted by the master registry as a prerequisite to the propagating.

Claim 28 (original): The system according to Claim 22, further comprising:

means for obtaining an identification of the trusted authenticating domain from the master registry.

Claim 29 (original): The system according to Claim 27, wherein the master registry stores trust policy information, and wherein the means for verifying that the trusted authenticating domain is trusted further comprises means for checking whether the stored trust policy information for the user includes the identification obtained from the user.

Claim 30 (original): The system according to Claim 27, wherein the master registry stores trust policy information, and wherein the means for verifying that the trusted authenticating domain is trusted further comprises means for checking whether the stored trust policy information for a

user group of which the user is a member includes the identification obtained from the user.

Claim 31 (original): The system according to Claim 28, wherein the master registry stores trust policy information, and wherein the means for obtaining the identification of the trusted authenticating domain from the master registry further comprises means for obtaining the identification using the stored trust policy information for the user.

Claim 32 (original): The system according to Claim 28, wherein the master registry stores trust policy information, and wherein the means for obtaining the identification of the trusted authenticating domain from the master registry further comprises means for obtaining the identification using the stored trust policy information for a user group of which the user is a member.

Claim 33 (original): The system according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret to the one or more other target registries further comprises means for identifying the one or more other target registries using the stored password synchronization policy information for the user.

Claim 34 (original): The system according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret to the one or more other target registries further comprises means for

identifying the one or more other target registries using the stored password synchronization policy information for a user group of which the user is a member.

Claim 35 (original): The system according to Claim 22, wherein the means for establishing the secure connection further comprises means for authenticating the PSA to the client.

Claim 36 (original): The system according to Claim 23, wherein the means for establishing the second secure connection further comprises means for authenticating the trusted authenticating domain to the PSA.

Claim 37 (original): The system according to Claim 24, wherein the means for establishing the third secure connection further comprises means for authenticating the master registry to the PSA.

Claim 38 (original): The system according to Claim 26, wherein the means for establishing additional secure connections further comprises means for authenticating the other target registries to the PSA.

Claim 39 (currently amended): The system according to Claim 22, wherein the means for validating further comprises:

means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

means for using the user identifier to locate a previously-stored identifying secret of the

user which was stored by the trusted authenticating domain; and

means for concluding that the validation succeeds if ~~comparing~~ the located identifying secret is identical to a result of performing the security function.

Claim 40 (original): The system according to Claim 22, wherein the means for validating further comprises means for invoking an authenticated LDAP bind or other native authentication mechanism of the trusted authenticating domain, wherein the identifier of the user and the identifying secret of the user are passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

Claim 41 (original): The system according to Claim 22, wherein the PSA has administrative authority for performing operations at the master registry.

Claim 42 (original): The system according to Claim 25, wherein the PSA has administrative authority for performing operations at the one or more other target registries.

Claim 43 (currently amended): A method for securely propagating security credentials using a trusted authenticating domain, comprising steps of:

establishing a secure connection between a client and a password synchronization agent (PSA);

transmitting an identifier of a user and an identifying secret of the user from the client to

the PSA over the secure connection;

validating the user with the trusted authenticating domain using the transmitted user identifier and identifying secret, on request of the PSA; and

propagating the identifying secret of the user directly from the PSA to a master registry if the validation succeeds.

Claim 44 (new): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining a new value fro the user to be used as the propagated identifying secret if the validation succeeds; and

computer-readable program code means for substituting this new value for the identifying secret prior to operation of the computer-readable program code means for propagating.

Claim 45 (new): The system according to Claim 22, further comprising:

means for obtaining a new value fro the user to be used as the propagated identifying secret if the validation succeeds; and

means for substituting this new value for the identifying secret prior to operation of the means for propagating.

Claim 46 (new): The method according to Claim 43, further comprising steps of:

obtaining a new value fro the user to be used as the propagated identifying secret if the validation succeeds; and

substituting this new value for the identifying secret prior to operation of the propagating

5 step.

as